

UNITED STATES PATENT AND TRADEMARK OFFICE
Docket No. 15065US01

In the Application of:

Wade Keith Wan, et al.

Electronically Filed on April 14, 2008

Serial No.: 10/642,318

Filed: August 15, 2003

For: PSEUDO-RANDOM NUMBER
GENERATION BASED ON PERIODIC
SAMPLING OF ONE OR MORE
LINEAR FEEDBACK SHIFT
REGISTERS

Examiner: Eleni A. Shiferaw

Group Art Unit: 2136

Conf. No.: 2849

PRE-APPEAL BRIEF REQUEST FOR REVIEW / SUBSTANCE OF INTERVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir / Madam:

This Pre-Appeal Brief Request for Review / Substance of Interview is being submitted in response to the Advisory Action mailed on February 7, 2008 and to the Interview Summary mailed on March 13, 2008. The Pre-Appeal Brief is being filed with a Notice of Appeal.

REMARKS / ARGUMENTS

GENERAL COMMENTS

The Advisory Action states the following:

Regarding argument references failure to disclose wherein "sampling output sequences of said linear feedback shift register with a specified periodicity," remark page 8, as recited in claim 1, argument is not persuasive because Meiyappan discloses a sampling switch that samples using LFSR output during periods when its sampling input line is active (see col. 3 lines 14-32 and fig. 2 element 206). Gressel discloses reducing the correlation between successive pseudo-random numbers by generating pseudo-random numbers using a linear feedback shift register and picking the numbers at specified clock periods (see 0046, 0096, abstract, 0026-0027 and 0097). Therefore, since the method in the reference performs the claimed step, it inherently achieves the same result of "in which the correlation between successive pseudo-random numbers is reduced;" Therefore applicant's arguments on page 10-13 as recited in claim 1 are not persuasive.

Regarding Applicant's argument in reference to claim 7, same argument as above applies to the alleged feature of "in which the correlation between successive pseudo-random numbers is reduced". Moreover, Furuta et al. discloses an LFSR register, random number generator, and a switching circuit to periodically switching [sic] between iterative outputs generated by at least a first LFSR and iterative outputs generated by at least a second LFSR and reducing the correlation between successive pseudorandom numbers (see col. 67 lines 36-col. 68 lines 2). Examiner respectfully submits that "this embodiment switches the connection of the switching circuit 1309 in response to the control signal after a predetermined number of bits are shifted in the LFSR 1302.", clearly anticipating "periodically switching", not after a time period per se, but after some action takes place.

Applicant's argument in reference to claim 11 is not persuasive because Thomas clearly teaches the claimed subject matter, as follows, "operating a nonlinear operator on said pseudo-random number and one or more operands" (claim 29, and par. 0213, and 0155, the two taps map to the one or more operands). See also claim 29. Applicant's arguments are not persuasive.

Applicant's argument wherein "varying the initial value of said hashing function over time by way of a function operating on one or more variables" as recited in claim 17, remark pages 18-20, is not persuasive because Walmsley teaches the use of time varying random number encrypted for the signature hash and verified see 0358-0365 and 0942-0943.

With respect to the first paragraph of the Advisory Action, the Examiner admits that "Meiyappan discloses a sampling switch that samples using LFSR output during periods *when* its sampling input line is active." Thus, the Applicant respectfully submits that Meiyappan (6993542) does not teach "sampling output sequences of said linear feedback shift register with a specified periodicity," as recited in Claim 1. As the Examiner indicates, Meiyappan discloses sampling of a linear feedback shift register only when the input line of a sampling switch is active, as illustrated in Figure 1, for example. As shown in Figure 1, the input line of the

sampling switch is the output of a bit reorder block. As evidenced at col. 3, lines 16-18, “Sampling switch 110 samples during periods when its sampling input line is active and does not sample when its sampling input is inactive.” Therefore, the input line is active only when the output of a bit reordering block is active. Therefore, Meiyappan does not disclose “sampling output sequences of said linear feedback shift register with a specified periodicity,” as recited in Claim 1. Consequently, for at least the foregoing reasons, the Applicants respectfully believe that Claim 1 contains patentable subject matter that should be allowed.

During an interview with the Examiner on March 3, 2008, the Examiner alleges that she briefly brought up one or more new references (e.g., 4905176, etc.) to back up the rejection of Claim 1. These references were not mentioned or cited in either the non-final Office Action (dated June 6, 2007) or the final Office Action (dated November 26, 2007). Since these new references were brought up by the Examiner in a conversation that occurred after Applicants’ response to the final Office Action, the Applicants believe that a rejection based on these new references at this juncture would constitute a new ground of rejection. Therefore, if the Examiner wishes to argue these new references after the final Office Action, the Applicants believe that these reference(s) should be properly cited (using a PTO 892 form) and argued in a new non-final Office Action.

In the Advisory Action and in the Office Actions, the Examiner alleges that “Gressel discloses reducing the correlation between successive pseudo-random numbers by generating pseudo-random numbers using a linear feedback shift register and picking the numbers at specified clock periods (0046, 0096, abstract, 0026-0027 and 0097). Furthermore, it appears that the Examiner has mischaracterized what is disclosed in Gressel when stating that Gressel discloses “generating pseudo-random numbers using a linear feedback shift register and picking the numbers at *specified clock periods*.” Applicants do not see any evidence that supports this statement after reviewing Gressel. As was stated by the Applicants in the Response (dated January 28, 2008), the Applicants maintain that Gressel, at paragraphs 0096, 0046, 0026-0027, 0097, and at the abstract, does not disclose what is recited in Claim 1. Applicants do not see how Gressel teaches “sampling output sequences of said linear feedback shift register with a *specified periodicity*,” as recited in Claim 1.” If the Examiner wishes to reject Claim 1 using Gressel, the Applicants request that the Examiner point out specific verbiage in Gressel that shows a teaching of each and every element recited in Claim 1. Therefore, Applicants believe that Claim 1 contains patentable subject matter that should be passed to allowance.

With respect to the second paragraph of the Advisory Action, the Examiner alleges that Furuta, at col. 67 lines 36-col. 68 lines 2, discloses what is recited in Claim 7. While Furuta, at col. 67, lines 36 - col. 68, lines 2, may disclose an embodiment that “switches the connection of the switching circuitry 1309 in response to the control signal after a predetermined number of bits are shifted in the LFSR 1302,” the Applicants respectfully submit that Furuta does not teach or disclose “periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register,” as recited in Claim 7. Nowhere does Furuta disclose anything about “periodically switching,” for example. Nor does Furuta disclose anything about periodically switching “between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register,” as recited in Claim 7. Furthermore, Figure 126 of Furuta discloses only *one* linear feedback shift register. Therefore, for at least the foregoing reasons, the Applicants believe that Claim 7 contains patentable subject matter. Rather than reference a rather large section of Furuta, at col. 67, line 36 – col. 68, line 2, the Applicants request the Examiner to specifically point out how there is a teaching of each and every element of what is recited in Claim 7.

The Interview Summary states that Furuta (5327522) teaches what is recited in Claim 7. Furthermore, the Examiner alleges that “Moreover the examiner provided other reference to show his invention is very well known as claimed (see Ooi USPN 5790666, col. 7 lines 5-35, fig. 2; PS signal generator 310...3LFSrs...switching signal 21...)”. In a similar note, Applicants respectfully submit that Ooi was not mentioned or cited in either the non-final Office Action (dated June 6, 2007) or the final Office Action (dated November 26, 2007). Since Ooi was brought up by the Examiner in a conversation which occurred after Applicants’ response to the final Office Action, the Applicants believe that a rejection based on Ooi would constitute a new ground of rejection. Therefore, if the Examiner wishes to argue a rejection using Ooi at this juncture, Applicants believe that these reference(s) should be properly presented (using a PTO 892 form) and argued in a new non-final Office Action.

With respect to the third paragraph of the Advisory Action, the Examiner alleges that Applicants’ argument is unpersuasive, without providing definitive evidence in Thomas to show a teaching of what is recited in Claim 11 and without addressing Applicants’ previous arguments in the Response dated January 28, 2008. As was argued by the Applicants in the Response dated January 28, 2008, the Applicants did not see how Thomas, at Claim 29, paragraphs 0213 and 0155, could possibly be used to show a teaching of “operating a nonlinear operator on said pseudo-random number and one or more operands,” as recited in Claim 11. The Examiner alleges that “the two taps map to the one or more operands.” However, the Applicants respectfully disagree. Instead, Claim 29 discloses “a first tap and a second tap for calculating a first value taken between the output of the first and second taps.” Thus, the first tap and second tap are simply used for calculating a first value, which is different from what is recited in Claim 11. Nowhere does Claim 29 disclose that two taps correspond or map to one or more operands of a non-linear operator, as alleged by the Examiner. Thus, based on what is disclosed in Thomas, the Applicants respectfully believe that the Examiner has improperly characterized what is disclosed in Thomas, when he alleges “the two taps map to the one or more operands.” Further, the Applicants respectfully submit that Thomas, at paragraph 0155 merely discloses that a first tap and a second tap of a linear feedback shift register are selected while Thomas, at paragraph 0213 does not provide a teaching of any element recited in Claim 11. In addition, the Examiner does not show “operating a nonlinear operator” on a “psuedo-random number *and* one or more operands,” as recited in Claim 11 (emphasis denoted in italics). Thus, for at least these reasons, Thomas does not teach what is recited in Claim 11. Consequently, the Applicants believe that Claim 11 contains patentable subject matter that should be passed to allowance.

In the Interview Summary, the Examiner states that “Regarding Claim 11, every single limitation is covered by the applied reference Thomas” The Examiner has maintained her rejection without addressing any of the Applicants’ previously submitted arguments that were presented in the Response dated January 28, 2008. Applicants respectfully submit that the Examiner has not properly shown a teaching of what is recited in Claim 11. Thus, the rejection to Claim 11 should be withdrawn.

With respect to the fourth paragraph of the Advisory Action, the Examiner alleges that “Walmsley teaches the use of time varying random number encrypted for the signature hash and verified see 0358-0365 and 0942-0943.” Applicants do not see how Walmsley, at paragraph 0360, provides any disclosure of an *initial value* of a hashing function as recited in Claim 17 (emphasis denoted in italics). Walmsley, at paragraph 0360, discloses a time varying random number; however, nowhere does Walmsley teach that this time varying random number is an initial value of a hashing function. Therefore, for at least this reason alone, Walmsley does not teach what is recited in Claim 17. Furthermore, the Office Action does not show a teaching of a “function operating on one or more variables,” as recited in Claim 17. Therefore, for at least

these reasons, Claim 17 is in condition for allowance. The Examiner has maintained her rejection without clearly providing supportive evidence that shows how Walmsley teaches what is recited in Claim 17. Applicants respectfully request the Examiner to address Applicants' arguments before concluding that Walmsley teaches what is recited in Claim 17. Applicants believe that Claim 17 contains patentable subject matter that should be passed to allowance.

In the Interview Summary, the Examiner has restated what was stated in the Office Actions. The Examiner has maintained her rejection without addressing any of the Applicants' previously submitted arguments as were presented in the Response dated January 28, 2008. Applicants respectfully submit that the Examiner has not shown a teaching of what is recited in Thus, the Applicants still believe that Claim 17 contains patentable subject matter.

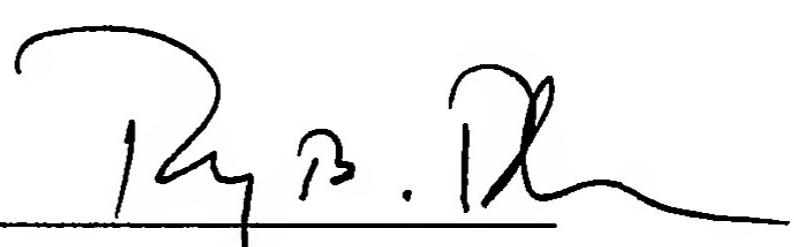
CONCLUSION

Applicants request the Examiner to consider and address the Applicants' arguments presented in this Pre-Appeal Brief / Substance of Interview. Applicants believe that the one or more pending claims are in condition for allowance. Therefore, the Applicants request that the Examiner indicate that these claims be advanced to allowance.

Because of the foregoing arguments presented by the Applicants, the pending claims should be passed to allowance. Furthermore, the Applicants request the Examiner to reference the Response dated 1/28/08, and to address all of the arguments presented by the Applicants in this Response with respect to the pending claims. Applicants respectfully requests that the Examiner show a teaching of each and every element recited in the pending claims by way of pointing out the verbiage that teaches each element in the pending claims. Otherwise, the Applicants believe that a Notice of Allowance should be provided by the Examiner.

Respectfully submitted,

Date: April 14, 2008

By: _____ 
Roy B. Rhee
Reg. No. 57,303

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
Telephone: (312) 775-8246
Facsimile: (312) 775-8100